

THE BUSINESS OF GOVERNANCE: CHINA'S LEGISLATION ON CONTENT REGULATION IN CYBERSPACE

ANNE S.Y. CHEUNG*

I. INTRODUCTION

The launch of the Internet in the early 1990s opened new frontiers, awakened new dreams, and offered new opportunities for many, but it also brought new challenges to ruling regimes and their subjects. Such challenges are exemplified in the case of China.

The Internet has given rise to a new generation of "netizens" in China who crave information. According to a survey by the China Internet Network Information Center (CNNIC), there are more than 100 million Internet users in China as of June 2005, a drastic leap from 620,000 when the CNNIC first carried out its survey in October 1997.¹ These netizens each spend more than one hour a day on the Internet, and 83.5% of them rated news as the most sought-after information.² Many netizens have turned chat rooms and bulletin board systems into an active virtual public sphere,³ and in some cases the Government has been forced to respond to discussions on such bulletin boards.⁴ Although the Internet is highly cen-

* Anne S.Y. Cheung is an associate professor at the Department of Law, University of Hong Kong. This Article was based on a conference paper presented at the *China and the Internet Conference* in Los Angeles in May 2003. It was later revised during her sabbatical leave at Tsinghua Law School, Beijing in 2005. The author would like to thank her research assistant Yang Lai, an outstanding student at Tsinghua Law School and one of the best students she has met.

1. CHINA INTERNET NETWORK INFORMATION CENTER, 16TH STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA 5 (2005), available at <http://www.cnnic.net.cn/download/2005/2005072601.pdf>; CHINA INTERNET NETWORK INFORMATION CENTER, STATISTICAL REPORT OF THE DEVELOPMENT OF CHINESE INTERNET 1 (1997), available at <http://www.cnnic.cn/download/manual/en-reports/1.pdf>.

2. *Id.* at 12, 17.

3. 40.6% accessed bulletin board systems and 20.7% accessed online chat rooms. *Id.* at 14.

4. The most notorious example is the school explosion in Jiangxi province in March 2001. The official explanation was that the explosion was

sored by the Chinese government, many speculate that its amorphous nature and the massive flow of information along the cyber highway will bring about a new kind of revolution, and may even bring democracy to China.⁵ While the Internet poses a threat to China's political leaders, the Chinese Communist Party (CCP) has a complicated position with regards to the Internet. The CCP desires the economic growth, prosperity, and investment opportunity that the Internet brings, but fears that the price that it pays for this economic wealth will be the downfall of its leadership.⁶ The major challenge for the CCP is therefore to attain the optimal level of information flow that is conducive to business transactions while preventing unfettered political or social discussion that could disrupt social stability and threaten state security.

Since 1996 the Chinese government has proposed widespread legislation to govern and monitor all aspects of the Internet, and the laws are often quickly introduced, revised, and

caused by a suicide bomber, but chat room and bulletin board discussions offered a different version that the primary school children had been forced to make firecrackers to subsidize the school's finances. Eventually, the government had to close down one of the most popular bulletin boards during that period. *See* Stephen Hsu, *Fight Over Net Freedom in China is Getting Ugly*, S. CHINA MORNING POST, Oct. 2, 2002, at 14. Another example is that the government has tightened its control over the online bulletin boards of universities since 2004. *See* Zhonggong zhongyang guo wu yuan fa chu Guan yu jin yi bu jia qiang he gai jin da xue sheng si xiang zheng zhi jiao yu de yi jian [St. Council Opinion on Further Strengthening and Improving the Political Thoughts and Education of University Students], PEOPLE's DAILY, October 15, 2004, <http://www.people.com.cn/GB/shizheng/1026/2920212.html> (last visited Feb. 7, 2006) (noting that the Internet can be an important tool in the improvement of the political education of university students). On March 16, 2005, the popular bulletin board of the prestigious Tsinghua University was closed to outsiders. *See* Wo lei chang liu: Chen tong dao nian shui mu Qinghua BBS [Cultural and Social Criticism—My Tears Flow Freely: In Loving Memory of Qinghua BBS], <http://www.philosophyol.com/bbs/printpage.asp?BoardID=34&ID=12429> (last visited Feb. 7, 2006).

5. *See* Xiao Qiang, *Cyber Speech: Catalyzing Free Expression and Civil Society*, HARVARD INT'L REV., Summer 2003, at 70-75; Jason Lacharite, *Electronic Decentralisation in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China*, 37 AUSTL. J. POL. SCI. 333-46 (2002).

6. *See* Kristina M. Reed, *From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce*, 13 TRANSNAT'L L. 451, 459-60 (2000).

reintroduced.⁷ In 2000 alone, six major regulations on Internet content control were promulgated by the National People's Congress,⁸ the State Council,⁹ and the Ministry of Information Industry,¹⁰ not including the various decrees that were announced by other ministerial units and regulations that were passed by provincial governments. This wave of legislation on content regulation continued into 2002.¹¹ The content of all sources of information is highly censored, and it is no surprise that the Chinese government only allows "politically correct" speech to be published on the Internet, meaning that pornography, violence, anti-government content, information that is harmful to the reputation and interests of the state, and expressions of ideas that undermine state religious policy are removed.¹² This policy is consistent with the Chinese communist style of governance that holds social stability paramount. What is more puzzling is that the nature of this

7. See, e.g., *Zhonghua renmin gonghe guo ji suan xin xi wang luo guo ji lian wang guan li zan xing* [Provisional Regulations of the People's Republic of China on the Management of International Networking of Computer Information Networks] (promulgated by the St. Council, Feb. 1, 1996, revised May 20, 1997, revised December 8, 1997), *LAWINFOCHINA* (last visited Feb. 17, 2006) (P.R.C.).

8. Decision of the Standing Committee of the National People's Congress Regarding the Maintenance of Internet Security (promulgated the Standing Comm. Nat'l People's Cong., Dec. 28, 2000), <http://www.chinaclaw.com/english/readArticle.asp?id=2386> (last visited Feb. 17, 2006) (P.R.C.) [hereinafter Standing Committee Decision on Internet Security].

9. E.g., *Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions* (promulgated by the St. Secrecy Bur., Jan. 25, 2000, effective Jan 1, 2000), *CHINALAWANDPRACTICE* (last visited Feb. 7, 2006) (P.R.C.) [hereinafter State Secrecy Provisions].

10. E.g., *Management Provisions on Electronic Bulletin Services on the Internet* (promulgated by the Ministry of Info. Indust., Nov. 6, 2000, effective Nov. 6, 2000), *LAWINFOCHINA* (last visited Feb. 17, 2006) (P.R.C.) [hereinafter Electronic Bulletin Services Provisions].

11. See, e.g., *Interim Provisions on the Administration of Internet Publication* (promulgated by the Ministry of Info. Indus. Apr. 27, 2002, effective Aug. 1, 2002), *LAWINFOCHINA* (last visited Feb. 17, 2006) (P.R.C.) [hereinafter Interim Internet Publication Provisions]; and *Regulations on the Administration of Business Sites of Internet Access Services* (promulgated by the St. Council, Sept. 29, 2002, effective Nov. 15, 2002), *LAWINFOCHINA* (last visited Feb. 17, 2006) (P.R.C.) [hereinafter Business Sites Regulations].

12. See Gudrun Wacker, *The Internet and Censorship in China*, in *CHINA AND THE INTERNET* 58, 62 (Christopher R. Hughes & Gudrun Wacker eds., 2003); and discussion *infra* Part III.A.

cluster of regulations is essentially consistent: they all govern the content of speech and reiterate the same forbidden grounds.¹³ One cannot help but ask why there is a need for this tide of seemingly repetitive legislation.

This paper explores the meaning and significance behind the flood of legislation that was introduced between 2000 and 2005 to regulate Internet content. I argue that the legislation represents an attempt to contract out responsibility to the business sector to accomplish the most effective monitoring of the Internet and to achieve the twin goals of power maintenance and economic growth in the midst of the globalizing effect of the Internet. In doing so, the CCP is also shaping the legal and business culture of the Internet. This paper also aims to map out the dynamic interplay between legislative control, the free flow of information, and the market in the age of the Internet and globalization.

It is tempting to dismiss this flood of legislation as a reflection of the Chinese government's frantic, piecemeal, and short-sighted effort to catch up with Internet technology. Various authors have, however, offered other theories to explain the phenomenon. David Cowhig sees the 2000 series as rehearsing the constant theme of power maintenance and social stability, and in his opinion the 2000 legislation has not added anything new to previous law but is merely an attempt to clarify the ambiguity in legislative style.¹⁴ Focusing on how content regulation affects the business sector, Clara Liang argues that the purpose of the legislation in 2000 was to favor the Chinese Communist Party and ensure that state-owned enterprises would be the first to benefit from Internet business competition.¹⁵ From the perspective of communication studies, Chin-chuan Lee argues that the 2000 legislation is an ideological affirmation of the party leadership in the face of China's entry into the World Trade Organization (WTO), and an attempt to "colonize the cyberspace by filling it up with a pre-

13. For a discussion of these laws, see *infra* part II.B.

14. See David Cowhig, *New Net Rules Not a Nuisance?*, CHINAONLINE NEWS, Dec. 5, 2000.

15. See Clara Liang, *Red Light, Green Light: Has China Achieved its Goals Through the 2000 Internet Regulations?*, 34 VAND. J. TRANSNAT'L L. 1417, 1417 (2001).

ponderance of government and enterprise Web sites.”¹⁶ Richard Cullen and D. W. Choy simply dismiss the 2000 legislation and its subsequent development as “old wine in a new bottle.”¹⁷

Using the recent scholarship and hindsight about the development of legislation on the Internet from 2000 to 2005, I argue that the series of legislation in 2000 and the further enactments in 2002 represent not merely repetition of the same theme or attempts at disambiguation, but represent instead the refinement of the broad concept of social stability. It is actually useful for the Chinese Communist Party to enact legislation that is vague and uncertain in nature. Only by doing this can it ensure ample room for interpretation and manipulation while holding its subjects in constant fear of offending the ruling regime, and under such conditions the likely reaction of the ruled is to self-censor even without being asked.¹⁸ Although it may be true that the Chinese Communist Party likes to ensure that economic benefits reach its own pocket and show special favoritism to state-owned enterprises,¹⁹ it has not been explained how different the case of Internet regulation is from the much-discussed phenomenon of *guanxi* (relationship or network) that is believed to be essential to establishing business ties, and that favors government officials’ interests, in China. Regardless of the ideological significance behind China’s Internet regulation, the impact of this legislation on the emerging economic and technological landscape is clear.

From 1996 to 2002, the Chinese government has gradually delegated its monitoring role to the business sector.

16. Chin-Chuan Lee, *The Global and the National of the Chinese Media*, in CHINESE MEDIA, GLOBAL CONTEXTS 15 (Chin-Chuan Lee ed., 2003).

17. Richard Cullen and D. W. Choy, *China’s Media: The Impact of the Internet*, 6 SAN DIEGO INT’L L. J. 323, 329 (2005).

18. Link has argued forcefully that vague and even self-contradictory laws are useful for the Chinese government, as they generate a culture of fear that results in the exercise of self-censorship on the part of the people. See Perry Link, *China: The Anaconda in the Chandelier*, N.Y. REV. OF BOOKS, Apr, 11, 2002, at 67, available at <https://www.nybooks.com/articles/15258> (last visited Feb. 17, 2006).

19. James Kynge, *Cancer of Corruption Spreads Throughout Country: SPECIAL SERIES AS BEIJING PREPARES FOR CRUCIAL PARTY CONGRESS AND CHANGE OF LEADERS PART FOUR: THE ALL-PERVERSIVE DISHONESTY*, FINANCIAL TIMES, Nov. 1, 2002, at 13.

Rather than merely imposing sanctions on individuals who voice “improper” opinions on the Web, Webmasters, operators of bulletin boards, owners of cybercafes, Internet service providers, Internet content providers, and portal companies all risk criminal sanctions for failing to censor “improper” speech.²⁰ This gradual shift of the burden of surveillance to the business sector may prove to be the most effective means for the Chinese authorities to control the Internet.

The drive to earn profits from the growth of the Internet has provided a solid base for a powerful coalition between the government and the business sector.²¹ China’s Ministry of Information Industry boasted in 2004 that the annual business volume of the Internet industry had topped RMB\$12.5 billion (about US\$1.6 billion), and was increasing at a rate of fifty percent a year.²² This is an alluring sum not only to the Chinese government, but also to foreign investors and local businessmen, and China’s entry into the WTO has only hastened the process of appeasement by foreign investors.

To capture these delicate dynamics, this paper is divided into three main parts. Part I discusses the nature of the Internet and the attempts of the Chinese government to control it. Part II comprises an analysis of legal control of the Internet in China before and after 2000. Part III examines the corresponding response of the business sector and details how investors have responded to the fears of the ruling regime, how they have been co-opted into various measures to allay these fears, and the conditions under which they resist them. In conclusion, this paper proposes that in the attempt to develop its economy and simultaneously control the flow of information, the socialist government has formed an unlikely partnership with investors. In this process of “cooperation,” much manipulation takes place on both sides.

20. See *infra* part III.C.

21. See, e.g., Thomas Crampton, *Google Puts Muzzle on Itself in China; Self-Censorship Seen as Cost of Business*, INT’L HERALD TRIB., Jan. 25, 2006, at 1.

22. *Diao cha xian shi: Zhongguo hu lian wang shi chang shou ru cheng zeng zhang tai shi* [*Statistics Show Revenue from China Internet Market is Increasing*], WEB NEWSLETTER FROM CHINA (Ministry of Info. Indus. / China Info. Indus. Net, Beijing, China), July 7, 2005, <http://www.cnii.com.cn/20050508/ca305233.htm> (last visited Feb. 7, 2006).

II. CHINA'S ATTEMPT TO CONTROL THE INTERNET: NAILING JELL-O TO THE WALL?

The advent of the Internet has brought hope to many. The dominance of Internet technology, the geographical distribution of its users, and the fluid nature of its content have led some to prophesize that this "Internet Holy Trinity"²³ will eventually bring a new era of e-revolution and e-democracy.²⁴ Bill Clinton, the former President of the United States, is known for his famous saying that the attempt to control the Internet is analogous to "nailing jell-o to the wall."²⁵

The beliefs of this group of cyber-optimists and enthusiasts are not unfounded. The Internet was originally designed with the aim of relaying U.S. command messages over a damaged network in the event of a nuclear war with the Soviet Union.²⁶ Thus, it was built as a distributed network with no central node or hierarchy, and the primary need was "survivability, flexibility and high performance."²⁷ Information is dispersed in small packets and is sent along numerous trajectories to be reassembled at the destination; computer users can store and share this information without the need for a single node or single server.²⁸ By its very design, the regulation of information flow on the Internet is meant to be difficult, if not impossible.²⁹

23. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, pt. I (1997), <http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm> (last visited Feb. 16, 2006).

24. See generally Lacharite, *supra* note 5; PIPPA NORRIS, *DIGITAL DIVIDE: CIVIC ENGAGEMENT, INFORMATION POVERTY, AND THE INTERNET WORLDWIDE* (2001).

R

25. Quoted in Kavita Menon, *Controlling the Internet: Censorship Online in China*, 88 *QUILL*, Sept. 2000, at 82.

26. Janet Abbate, *INVENTING THE INTERNET* 8-13 (1999).

27. *Id.* at 5.

28. The predecessor to the Internet was the ARPANET, which was created and funded by the US Department of Defense's Advanced Research Project Agency. The experiment started in the Cold War period in the 1960s, but it was not until the 1970s that the the network was developed for commercial exploitation. Gradually, it expanded into an increasingly commercial communication system. For an account of the historical context and development of the ARPANET and the Internet, see *id.* at 8.

29. See Paul Callister, *The Internet, Regulation and the Market for Loyalties: An Economic Analysis of the Transborder Information Flow*, 2002 U. ILL. J.L. TECH. & POL'Y 59, 62-81 (2002).

The unbounded potential of the Internet naturally causes concern to authoritarian government regimes, and China is a prime example. Realizing the benefits that the new age of information technology will bring, China has eagerly embraced the Internet. But China is equally anxious to limit its benefits to economic development, and any spillover effect into the political public sphere is perceived as a threat to social stability and order.

The main method of control that has been adopted by the Chinese government is restriction of access to the Internet. China has attempted to mark a division between “global cyberspace” and “domestic cyberspace”³⁰ by building a virtual firewall, which is the largest filter and blocking system in the world. At the national level, only nine government-approved agencies are permitted to establish an Internet Interconnecting network and to license the operation of Internet service providers.³¹ These nine networks are, in turn, required to go through international gateways controlled by the Ministry of Information Industry that are located in the three cities of Beijing, Shanghai, and Guangzhou. No individual or group is allowed to establish a direct international connection, and the primary entry and access points to Chinese cyberspace are strictly controlled.³² This structure arguably provides the basis for an intranet—or an internal network that can be shut off

30. Jack Linchuan Qiu, *Virtual Censorship in China: Keeping the Gate between the Cyberspaces*, INT'L J. COMM. L. & POL'Y, Feb. 13, 2000, at 2.

31. The major Internet Interconnecting networks are CSTNET, which is owned by the Chinese Academy of Science; CHINANET, which is owned by China Telecom; UNINET, which is owned by China Unicom; CNCNET, which is owned by China Netcom; CERNET, which is owned by the State Educational Commission; CMNET, which is owned by China Mobile; CSNET, which is owned by ChinaSat; CIETNET, which is owned by the China International E-Trade Centre; and CGWNET, which is owned by the China Great Wall Group. Information from China Internet Network Information Centre, *17th Statistical Report on the Internet Development in China* at 9 (Jan. 2006) at <http://www.cnnic.net.cn/download/2006/17threport-en.pdf>. For information on ownership of network operators, see *A Brief Introduction to the Ten Major Network Operators (Shi Da Hu Lian Wang Dan Wei Jian Jie)* at <http://www.cnnic.net.cn/html/Dir/2003/11/17/1330.htm>. In 1996 there were only four major interconnecting networks. See J. Mike Rayburn and Craig Conrad, *China's Internet Structure: Problems and Control Measures*, 21 INT'L J. OF MANAGEMENT 471, 472-73.

32. See Zixiang A. Tan, *Regulating China's Internet: Convergence Toward a Coherent Regulatory Regime*, 23 TELECOMM. POL'Y 261, 270-72 (1999).

from the outside world—and a firewall, which is a system of Internet blocks and filters that intercepts access by users to politically undesirable and objectionable materials.³³ This system is structured as a four-tier pyramid with the Ministry of Information Industry controlling the government gateway at the top level, followed by government Internet service providers managing all interconnecting networks and installing filters to block away undesirable content, coupled with the cooperation of registered private sector Internet service providers, and all Internet users under control.³⁴ This is a relatively efficient and effective means of control. According to a study by Harvard University's Berkman Center for the Internet and Society in 2003, a tenth of Internet sites are inaccessible in China.³⁵ At various points in time and depending on the region, sites that have been blocked include *The Economist*, *Cable News Network*, and *The New York Times*.³⁶

Nevertheless, control over the flow of information on the Internet is hardly foolproof. The use of technology to block sites is followed by counter-blocking and counter-filtering technologies to evade the censorship. Different authors have written about how to bypass the systems and how to use proxy servers to break through the various barriers.³⁷ Anti-blocking software, mirror sites, remailers, secret Usenet groups, and anonymous e-mail services have all made enforcement difficult.³⁸ Guerrilla warfare is constantly being waged between the Chinese government and high-tech libertarians.

33. Cf. S. David Cooper, *The Dot.Communist Revolution: Will the Internet Bring Democracy to China?*, 18 UCLA PAC. BASIN L.J. 98, 105 (2000) (discussing the intranet idea and filtering of websites).

34. J. Mike Rayburn & Craig Conrad, *China's Internet Structure: Problems and Control Measures*, 21 INT'L J. MGMT. 471, 472-73 (2004).

35. Study: *One-Tenth of Internet Sites May Be Blocked in China*, WORLD IT REP., Apr. 10, 2003, at 1. The Berkman Center tested 200,000 Web sites. For the report, see JONATHAN ZITTRAN & BENJAMIN EDELMAN, BERKMAN CENTER FOR INTERNET & SOC., EMPIRICAL ANALYSIS OF INTERNET FILTERING IN CHINA, (2003), <http://cyber.law.harvard.edu/filtering/china/>.

36. See *id.*; Ronald J. Deibert, *Dark Guests and Great Firewalls: The Internet and Chinese Security Policy*, 58 J. SOC. ISSUES 143, 147 (2002).

37. Famous anti-censorship software includes Triangle Boy and Freenet China. See Jennifer 8. Lee, *Guerrilla Warfare, Waged with Code*, N.Y. TIMES, Oct. 10, 2002, at G1. For a discussion of anti-censorship technologies, see Lacharite, *supra* note 5, at 339.

38. Lacharite, *supra* note 5, at 339-41.

Jason Lacharite further points out that the clumsy bureaucratic structure of the Chinese government has made control over Internet communication simply impractical and selective censorship impossible in many cases.³⁹ In 1999, there were fifteen-thousand individual criminal violations on the Internet, but only two major cases were prosecuted by the Public Security Bureau.⁴⁰ Moreover, despite the existence of criminal sanctions, it is common to use the Internet to expose the corrupt behavior of local officials.⁴¹ It is not surprising that, as will be illustrated in the following discussion, the Chinese government has resorted to building an “empire of regulations”⁴² that will combine direct and indirect control in an attempt to purge any “pollution” from the Internet.

III. CHINA’S LEGAL REGIME TO REGULATE THE INTERNET: BUILDING A PANOPTICON IN CYBERSPACE

Historically, stringent formal standards are not the most effective form of control and censorship. Long before the invention of the Internet, Jeremy Bentham proposed the construction of a mighty Panopticon in which prisoners would live under the omnipresent gaze of the ruler without knowing when they were being observed.⁴³ In the modern era, Michel Foucault, although not speaking in the context of cyberspace, refined Bentham’s theory of control to present a vision of surveillance and discipline from both state and non-state actors in our daily lives. According to his theory, power is most effectively exercised when an entire society participates in surveillance at all institutional levels.⁴⁴ Recently, James Boyle, speaking directly about the Internet, elaborated that the most effective and cost-efficient scheme of control is a design that combines criminal sanctions with privatized enforcement.⁴⁵

39. *Id.* at 334.

40. *Id.* at 336.

41. See Benjamin L. Liebman, *Watchdog or Demagogue? The Media in the Chinese Legal System*, 105 COLUM. L. REV. 1 (2005).

42. Deibert, *supra* note 36, at 147.

43. See MICHEL FOUCAULT, *DISCIPLINE AND PUNISH* 200-209 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1978); see generally JEREMY BENTHAM, *THE PANOPTICON WRITINGS* (Miran Bozovic ed., 1995).

44. *Id.* at 216-17.

45. Boyle, *supra* note 23.

Building on this bifurcated scheme of direct control and censorship by the state, and indirect discipline and surveillance by non-state actors, the Chinese government has successfully created a culture of self-censorship not only among its citizens, but also by co-opting local and foreign investors. These capitalists duly comply with the general wishes of the government, and also act on its behalf as non-state actors. The development of this control mechanism can be traced by studying the legal regulations in China from 1993 onward. While the major characteristic of the legal regulations that were passed between 1993 and 1999 was a heavy reliance on direct censorship on the part of government agents, the legislation from 2000 onward has been characterized by the increasing delegation of policing power to non-state actors.⁴⁶ The business sector in particular is now shouldering the responsibility of surveillance and reporting.⁴⁷

One could arguably say that this trend is not exclusive to China because both the United States and Europe have enacted legislation to regulate Internet content through intermediaries. However, it is important to note that China has imposed general and all-encompassing obligations on *all* intermediaries, whereas the U.S. and European models are based on a “notice and take down” regime. For example, according to the U.S. Digital Millennium Copyright Act, Internet service providers are generally not liable for copyright infringement.⁴⁸ However, once notification of alleged copyright violation has been given to an Internet service provider, it must remove the materials “expeditiously” in order to avoid liability.⁴⁹ Subscribers may provide counter-notice to the Internet service provider and obtain reinstatement of the allegedly infringing material.⁵⁰ Under article 14 of the European

46. See Zixiang (Alex) Tan, Milton Mueller, & Will Foster, *China's New Internet Regulations: Two Steps Forward, One Step Back*, 40 COMM. OF THE ACM 11, 13-14 (1997), available at <http://som.csudh.edu/fac/lpress/devnat/nations/china/chinah.html>; OPENNETINITIATIVE, Internet Filtering in China in 2004-2005: A Country Study (Apr. 14, 2005), http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf.

47. See Internet Filtering in China in 2004-2005: A Country Study, *supra* note 46.

R

48. 17 U.S.C. § 512(c) (1998).

49. *Id.* Such notice must meet several requirements. 17 U.S.C. § 512(c)(3).

50. 17 U.S.C. § 512(g).

Union Directive on Electronic Commerce of June 8, 2000, a hosting provider is not liable for the information that is stored at the request of a client, provided that the service provider does not have actual knowledge of the information.⁵¹ However, once the service provider has notice of illegal activity, it must act expeditiously to remove or disable the information.⁵²

A. 1993-1999: *Regime of Direct Control*

During the initial stage of Internet development in China, the major concerns of the government were to control access to information and to censor undesirable information through the most direct means available.

The *Temporary Regulation for the Management of Computer Information Network International Connection* was passed on January 23, 1993,⁵³ and laid down the ground rules for all Internet users, stipulating that no entities or individuals were allowed to establish a direct international connection by themselves. All users had to register to gain access to the Internet, and anyone who provided Internet access to users had to obtain a license.

This supervision framework was supported by managerial measures from what were then the four major networks. Technicians were employed in the daily maintenance of cyberspace, and systems operators, Webmasters, and board administrators were recruited to scrub messages from the Internet.⁵⁴

The content that is allowed on the Internet in China has always been strictly regulated. On February 18, 1994, the *Order for Security Protection of Computer Information Systems* was issued by the State Council.⁵⁵ The Ministry of Public Security subse-

51. Council Directive 2000/31, art. 14, 2000 O.J. (L 178) 1, 13 (EC).

52. For details, see Benoit Frydman & Isabelle Rorive, *Regulating Internet Content through Intermediaries in Europe and the USA*, 23 *ZEITSCHRIFT FÜR RECHTSSOZIOLOGIE* 41 (2002), available at http://www.droit-technologie.org/2_1.asp?dossier_id=99 (last visited Feb. 17, 2006).

53. It was formally announced through the Interim Regulations on the Management of International Networking of Computer Information (promulgated by the St. Council, Feb. 1, 1996, amended and effective May 20, 1997), *LAWINFOCHINA* (last visited Feb. 6, 2006) (P.R.C.). For a further discussion see Qiu, *supra* note 30, at 10.

54. See Qiu, *supra* note 30, at 14-15.

55. Regulations of the People's Republic of China for Safety Protection of Computer Information Systems (promulgated by the St. Council, Feb. 18, 1994, effective Feb. 18, 1994), <http://ce.cei.gov.cn/elaw/law/lb94b1e.txt> (last visited Feb. 17, 2006) (P.R.C.).

quently became responsible for Internet security and protection, the management of computer information networks and the investigation of any illegal cases. The *Order* was confirmed on December 11, 1997, when the Ministry of Public Security issued its *Computer Information Network and Internet Security Protection and Management Regulations (1997 Regulations)*.⁵⁶ Under article 6 of the *1997 Regulations*, all Internet and network users had to gain prior approval from the Ministry of Posts and Telecom before using the Internet, adding information to or deleting information from the Internet, or changing network functions. Under article 11, all Internet users had to provide their personal information and identification when applying for Internet access; the information would be kept by the police.

Prohibited content on the Internet was also laid out in article 5 of the *1997 Regulations*.⁵⁷ Essentially, the forbidden list for Internet publication is the same as for the printed media.⁵⁸ Despite later developments in Internet regulations, the content on this list has remained essentially the same. The production, duplication, release, and dissemination of content in nine categories are absolutely forbidden.⁵⁹ Information that:

56. Computer Information Network and Internet Security, Protection and Management Regulations (approved by the St. Council, Dec. 11, 1997, promulgated by the Min. Pub. Security, Dec. 30, 1997), http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law_security.pdf (last visited Feb. 17, 2006) (P.R.C.).

57. *Id.* art. 5.

58. For instance, article 300 of the 1997 Criminal Law stipulates that whoever utilizes superstition to undermine the implementation of the laws and administrative rules and regulations of the State is to be sentenced to not less than three years and not more than seven years of fixed-term imprisonment. Criminal Law [Crim. L.] (promulgated by the Standing Comm. Nat'l People's Cong., Mar. 14, 1997, effective Oct. 1, 1997) art. 300, LAWINFOCHINA (last visited Feb. 17, 2006) (P.R.C.) (according to lawinfochina.com this version of the law has expired). It is also a crime to subvert the government or to overthrow the socialist system. *Id.* art. 105. Other articles criminalize the dissemination of pornographic materials. *Id.* arts. 363-64.

59. See, e.g., Interim Provisions on the Administration of Internet Culture, (promulgated by the Min. Cult., May 10, 2003, effective July 1, 2003) art. 17, LAWINFOCHINA (last visited Feb. 6, 2006) (P.R.C.); Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network (promulgated by the St. Admin. Radio,

- is contrary to the basic principles that are laid down in the Constitution, laws or administration regulations;
- is seditious to the ruling regime of the state or the system of socialism;
- subverts state power or sabotages the unity of the state;
- incites ethnic hostility or racial discrimination, or disrupts racial unity;
- spreads rumors or disrupts social order;
- propagates feudal superstitions; disseminates obscenity, pornography or gambling; incites violence, murder or terror; instigates others to commit offences;
- publicly insults or defames others;
- harms the reputation or interests of the State; or
- has content prohibited by laws or administrative regulations,

is forbidden to be disseminated or expressed on the Internet.⁶⁰ In 2002 one more area—"harming the social morality or the excellent cultural traditions of the nationalities"—was added.⁶¹ In total, the ten forbidden categories have set the framework for subsequent legislation on Internet content regulation in China.⁶²

To further regulate information security, the Administration of Commercial Encryption Regulations (Encryption Regulations) were passed by the State Encryption Management Commission (SEMC) in 1999.⁶³ Under the Encryption Regu

Film & Telev., July 7, 2004, effective Oct. 11, 2004) art. 19, LAWINFOCHINA (last visited Feb. 6, 2006) (P.R.C.).

60. The classification of information in China depends on various pieces of legislation. The examples of superstition and subversion are governed under the Criminal Law, discussed *supra* note 58. For an overview of the regulatory bodies, the relevant statutes, and classification of information, see generally H.L. FU & RICHARD CULLEN, MEDIA LAW IN THE PRC (1996).

61. *See* Interim Internet Publication Provisions, *supra* note 11, art. 17(9); Business Sites Regulations, *supra* note 11, art. 14(9).

62. *See, e.g.*, Interim Provisions on the Administration of Internet Culture, *supra* note 59, art. 17; Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network, *supra* note 59, art. 19.

63. Administration of Commercial Encryption Regulations (promulgated by the St. Council, Oct. 7, 1999, effective Oct. 7, 1999) CHINALAWANDPRACTICE (last visited Feb. 7, 2006) (P.R.C.) [hereinafter Encryption Regulations].

R

R

R

R

lations, the production, sale, use, and research⁶⁴ of products that contain commercial encryption codes are subject to filing, certification, and approval requirements. Foreign entities or individuals that use encryption products or equipment that contains encryption technology within China must report these products and their usage to the SEMC to obtain approval. As commercial encryption technology is regarded as a state secret under article 3, regulation also falls under the *Law of the People's Republic of China on Guarding State Secrets*.⁶⁵

The scope of the *Encryption Regulations* is so broad and the requirements so stringent that they even cover Lotus and Microsoft office suites. Although the Chinese government narrowed the scope of the *Regulations* after protests from foreign investors,⁶⁶ the *Regulations* reflect how ambitious and careful the government has been to gain control of and monitor every corner of the Internet.⁶⁷

To facilitate management and control, the government has also streamlined its structure. Before 1998, the Ministry of Post and Telecom was the designated regulator and had a de facto monopoly of China's telecommunications services, overseeing its postal services, telecommunications, and telegraph and wire services. The Ministry of Electronic Industry was responsible for making decisions about the manufacture of information-technology products and was the largest manufacturer in China. It laid down policies, conducted research, and produced telecoms equipment. The two ministries competed to play a leading role in the telecommunications and Internet industry,⁶⁸ but in 1998 they were merged to form the Ministry of Information Industry. The Ministry of Information Industry became the primary regulator of China's telecom and Internet

64. See *id.* arts. 7, (production), 11 (sale), 14-16 (use), & 15, 17 (research).

65. Law on Guarding State Secrets (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 5, 1988, effective May 1, 1999), LAWINFOCHINA (last visited Feb. 6, 2006) (P.R.C.).

66. This point will be further elaborated in Part III of the paper.

67. For further discussion of the *Encryption Regulations*, see Hu Zaichi, *Commercial Encryption Regulation*, INT'L INTERNET L.REV., Apr. 2000, at 33; *China's Internet: an Uncertain Future*, CHINA L. & PRAC. (Mar. 2000), available at 2000 WLNR 264439 (Westlaw).

68. See Tan, *supra* note 32, at 266-70 (detailing restructuring of the government departments).

sectors, with responsibility for overall planning and administration and the issuing of operating licenses to telecom operators and Internet service providers.⁶⁹

B. Post-2000 Regime: An Era of Delegated Control

The pre-2000 style of Internet regulation was top-down, hierarchical, and direct. In contrast, the legislation from 2000 till the present marked a new style of ruling through delegation, self-monitoring, and self-censorship. In 2000 alone, six major pieces of regulation were enacted:

Promulgation Date in 2000	Issuing Authority	Legislation or Regulations
January 25	State Secrecy Bureau	Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions (State Secrecy Provisions) ⁷⁰
September 1	State Administration of Industry and Commerce	Interim Procedures on the Regulation and Filing of Online Business Operation ⁷¹
September 25	State Council	Regulation on Internet Information Service of the People's Republic of China ⁷²
October 8	Ministry of Information Industry	Management Provisions on Electronic Bulletin Services in the Internet (Electronic Bulletin Services Provisions) ⁷³

69. *See id.* (describing in detail the consolidation of Chinese government control over the Internet into a single central administrative body during the 1990s).

70. *See* State Secrecy Provisions, *supra* note 9.

R

71. Jing ying xing wang zhan bei an deng ji guan li zan xing ban fa [Interim Procedures on the Regulation and Filing of Online Business Operation] (promulgated by the St. Admin. Indus. & Commerce, Sept. 1, 2000, effective Sept. 1, 2000) <http://www.gxhd.com.cn/newgxhd/xuzhi/glbf.htm> (last visited Feb. 08, 2006) (P.R.C.).

72. Regulation on Internet Information Service (promulgated by the St. Council, Sept. 25, 2000, effective Sept. 25, 2000), LAWINFOCHINA (last visited Feb. 17, 2006) (P.R.C.).

73. *See* Electronic Bulletin Services Provisions, *supra* note 10.

R

November 7	Press Office of the State Council and Ministry of Information Industry	Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions (Internet News Publication Provisions) ⁷⁴
December 28	Standing Committee of the National People's Congress	Decision of the Standing Committee of the National People's Congress Concerning Maintaining Internet Security (National People's Congress Security Law) ⁷⁵

Various commentators have interpreted this sudden rush of legislation as an affirmation of the leadership by the CCP, an ideological declaration, an attempt to exert control in the wake of China's entry into the WTO, or as an attempt by the CCP to maintain its vested economic interest in state-owned or sponsored enterprise.⁷⁶ A quick preview of the titles reveals that four of the six pieces of legislation are aimed at the business sector. Liang sums up the features of the 2000 regulations as either informational or economic: informational in the sense that the regulation of content control is the prime concern, and economic in the sense that they affect business operations in China.⁷⁷

In terms of informational or content control, the state has been consistent in its strict style of censorship to ensure security, as is demonstrated in article 15 of the *Regulation on Internet Information Services of the People's Republic of China*, article 13 of the *Internet News Publication Provisions*, article 9 of the *Electronic Bulletin Services Provisions*, and articles 2, 3, and 4 of the *National People's Congress Security Law*. Under the latter, the disclosure of state, intelligence, or military secrets through the Internet is specifically prohibited (article 2(2)), using the Internet to organize a cult or to keep in touch with cult members is banned (article 2(4)), and the fabrication of false information that affects securities and futures trading is also forbidden

74. *Hu lian wang zhan cong shi deng zai xin wen ye wu guan li zan xing gui ding* [Provisional Regulations for the Administration of Websites Engaged in the Publication of News] (promulgated by the St. Council, Nov. 7, 2000), <http://w.5isobu.com/policy/39001272004414151082010101859.html> (last visited Feb. 17, 2006) (P.R.C.).

75. Standing Committee Decision on Internet Security, *supra* note 8.

76. Discussed *supra*, in Introduction.

77. See Liang, *supra* note 15, at 1418. Liang examines only the Measures for Managing Internet Information Services and Interim Procedures on Regulation and Filing of Online Business Operation.

R

R

(article 3). Arguably, these three categories already fall within the nine forbidden content categories that were laid out in the 1997 *Computer Information Network and Internet Security Protection and Management Regulations*.⁷⁸

Content control on the Internet is supplemented by the *State Secrecy Provisions*. Article 7 of the *Provisions* states that no information concerning state secrets, including state confidential information that is approved for distribution to designated overseas recipients, may be stored, processed, or transmitted via computer systems with Internet access. However, the term “state secret” is not defined under the *Provisions*. This ambiguity is consistent with the Chinese style of ruling that leaves room for the regime to manipulate the law. State secrets could refer to almost any information that is not officially approved for publication and disclosure, and citizens thus are expected to behave lest sanctions be imposed.

What marks a difference in the style of ruling is that the scope of the *State Secrecy Provisions* is broad, and one may be held to be “vicariously liable” for activities that happen within one’s realm of “control.”⁷⁹ All individuals, corporations, and other organizations that use the Internet are subject to the *Provisions*.⁸⁰ Under article 8, a person who places information on the Internet shall be ultimately liable for any unlawful dissemination of that information, although information that is provided to or released on Web sites must be checked and approved by the appropriate government department anyway. All of the national backbone networks, Internet service providers, and users must establish management systems to protect secret information. Under article 9, all online posting must obtain prior approval from the content provider pursuant to an internal secrets protection procedure. Under article 10, all entities or users that establish online bulletin board systems, chat rooms, or network news groups are subject to examination and approval by the relevant government agencies. Under chapter 3, providers of Internet service and content are

78. Cf. *Computer Information Network and Internet Security, Protection and Management Regulations*, *supra* note 56 (covering prohibition against disclosing government secrets).

R

79. *State Secrecy Provisions*, *supra* note 9, art. 10.

R

80. *Id.* art. 3.

held liable for any failure to monitor and supervise electronic activities that are conducted within their business sphere.

Internet service and content providers themselves are regulated directly by the *Regulation on Internet Information Services of the People's Republic of China*, which is specifically directed at "Internet information service providers (IISPs),⁸¹ defined to refer to [the] activity of providing information services to online users by means of the Internet" (article 2). The term "Internet information service providers" covers both the operational and the non-operational sectors (article 3). The former refers to providers who charge, and are therefore liable to apply for a license. The latter refers to providers of public and shared information to online users free of charge, which must file applications. This means that Internet content providers and portals such as Yahoo! fall under the *Regulation*. All providers that offer news and publish and supply information about: education; medication, health care, and pharmaceutical products; medical apparatus; and instruments are further required to obtain approval from the relevant regulatory departments (article 5). The general rule is that all IISPs are required to provide online users with quality services and to ensure the "legality" of the information that is provided under article 13. Under article 14, IISPs that offer news coverage and bulletin board services are required to keep a sixty-day record of the information that they distribute, when it is distributed, and the Web address where the information is located. IISPs are similarly required to keep records of the time of use, accounts of Internet addresses or domain names, and dial-in telephone numbers of online users for 60 days. The *Regulations* are considered to be the prime model for the strict control of Internet administration.⁸²

Similarly, the *Electronic Bulletin Services Provisions* also require electronic bulletin service providers to keep a record of users (article 14 and 15), monitor their activities (article 6), and report any violations to the authorities (article 13). The *Provisions* cover the release of information through online in-

81. Administrative Measures on Internet Information Services (promulgated by the St. Council, Jan. 25, 2000, effective Sept. 24, 2000) art. 2 CHINAITLAW (last visited Mar. 20, 2006) (P.R.C.).

82. Jingzhou Tao & Taili Wang, *Net Laws Prepare China for WTO Entry*, INT'L INTERNET L. REV., Apr. 2001, at 23, 25.

teractive forums, including electronic bulletin boards, electronic white boards, Internet forums, online chat rooms, and message boards (article 2). Article 3 specifically requires service providers to “strengthen self-regulation.”

The *News Publication Provisions* place strict limitations on online news. The *Provisions* apply to Internet sites that engage in the business of news publication on the Chinese mainland, and also cover the release and republication of news on the Internet (article 2). These *Provisions* clearly stipulate that without specific approval, Web sites are prohibited from linking to foreign news Web sites or disseminating news from the foreign news media or Web sites (article 14). Only news that has been published on the Internet by the official state-owned media or the news departments of the state institutions themselves, or has already been published by authorized media in another form can be posted on the Internet (articles 5 and 7). In other words, Internet portals like Sina, Netease, and Sohu are required to exercise self-censorship.⁸³

Thus, in the post-2000 legislation, the government indirectly regulates access to content on the Internet by directly regulating intermediary actors, such as Internet service and content providers. If Internet service or content providers discover prohibited content, they are obligated to cease transmission of the information, keep records of the Internet users concerned (including account number, identity, telephone number, domain names, and information posted), and report the information to the relevant authorities. Failure to do so may result in a temporary or permanent suspension of the site. They may also face a fine of up to RMB\$1 million (approximately US\$128,000) or imprisonment.⁸⁴ Thus, the *Provisions* impose an obligation on service providers to monitor and report the activities of their users, an obligation that Wacker

83. Wacker argues that the *News Provisions* have both ideological and economic dimensions that facilitate control and ensure that the economic interests of the Internet are in the hands of state-owned enterprise. *See* Wacker, *supra* note 12, at 58, 63.

84. In general, this is governed under articles 19 to 23 of the Regulation on Internet Information Service, *supra* note 72. For example, article 20 of the Electronic Bulletin Services Provisions also stipulates that providers of electronic bulletin services who violate the provisions shall be punished in accordance to articles 21 and 23 of the Regulation on Internet Information Service. *Id.*

compares to holding the postal service liable for the contents of the letters and parcels that it accepts for transportation and delivery.⁸⁵

C. Post-2000 Governance: A Regime of Regulation, Co-Regulation, and Self-Regulation

Other than holding individuals criminally liable for their expression, Internet information service providers also face criminal sanctions for the publication of prohibited content. Draconian as it may sound, regulation, co-regulation, and self-regulation became the prevailing style of rule after 2000. In 2001, Internet cafes came under regulation through the *Measures on the Administration of Business Sites of Internet Access Services (2001 Measures)*.⁸⁶ Although the major target of the *Measures* was the growing business of Internet cafes, places of business that were also covered by the 2001 *Measures* included Internet bars, computer lounges, and other places that provide Internet access to the public through computers and like devices.⁸⁷ The 2001 *Measures* were replaced by the *Regulations on the Administration of Business Sites of Internet Access Services*, which were passed by the State Council on September 29, 2002.⁸⁸ The owners of such businesses are required to install tracking software, institute surveillance and monitoring measures, and report to the relevant authorities if a user employs the Internet for illegal activities (article 19). Operators must keep the records of each user's identity card and Internet usage for no fewer than sixty days (article 23), and such businesses are required to be located a minimum of two hundred meters from residential areas and primary and secondary

85. Gudrun Wacker, *Behind the Virtual Wall: The People's Republic of China and the Internet*, in CONTEMPORARY CHINA : THE DYNAMICS OF CHANGE AT THE START OF THE NEW MILLENNIUM 127, 145 (P.W. Preston & Juergen Haacke eds., 2003).

86. Measures on the Administration of Business Sites of Internet Access Services (promulgated by the Ministry of Info. Indus. & Com., Apr. 3, 2001, effective Apr. 3, 2001), LAWINFOCHINA (last visited Feb. 17, 2006) (P.R.C.).

87. Business sites of Internet access services mean the "sites of a profit-making nature which provide the public with Internet access services through computer and networking of Internet." *Id.* art. 2. This definition is further elaborated under Business Sites Regulations, *supra* note 11, art. 2 (defining business sites of Internet access services to be "sites of a profit-making nature, such as network bars, computer lounges etc").

88. Business Sites Regulations, *supra* note 11.

schools.⁸⁹ The hours of operation are limited to eight in the morning to midnight (article 22), and minors may not enter (article 21). Statistics show that at the end of 2000, there were 22.5 million Internet users in China, 20.5% of whom frequented Internet cafes or similar places of business.⁹⁰ In setting up this system of self-surveillance, the government has covered a sizable population of netizens, and subsequent policy statements in 2004 reflected the call for this spirit of "self-enforcement" and "self-discipline by the industry."⁹¹ From the enactment of the *Administration of Places of Business for the Provision of Internet Access Services Regulations* to early 2004, the number of Internet cafes and places of business that provided Internet access dropped by almost half from approximately 200,000 to 110,000.⁹² Those that are still in operation must

89. *Id.*, art. 9. The Ministry of Culture further prohibits the running of such establishments near secondary schools. *Wenhua bu guan yu guan che "Hu lian wang shang wang fu wu ying ye chang suo guan li tiao li" de tong zhi* [Notice on the Implementation of the Regulations on the Administration of Businesses Providing Internet Access Services] (promulgated by the Min. Cult., Oct. 11, 2002), ¶ 2, <http://w.51sobu.com/policy/39021111200441311080796166484.html> (last visited Feb. 13, 2006) (P.R.C.), citing *Hu lian wang shang wang fu wu ying ye chang suo guan li tiao li* [Regulations on the Administration of Businesses Providing Internet Access Services] (promulgated by the St. Council, Sept. 29, 2002, effective Nov. 15, 2002), <http://w.51sobu.com/policy/390210292004315251080198530171.html> (last visited Feb. 13, 2006) (P.R.C.).

90. See CHINA INTERNET NETWORK INFORMATION CENTER, SEMIANNUAL SURVEY REPORT ON THE DEVELOPMENT OF CHINA'S INTERNET (2001), <http://www.cnnic.net.cn/download/manual/en-reports/7.pdf> (last visited Feb. 17, 2006).

91. *Guo wu yuan ban gong ting zhuan fa Wenhua bu deng bu men guan yu kai zhan wang ba deng hu lian wang shang wang fu wu ying ye chang suo zhuan xiang zheng zhi yi jian de tong zhi* [State Council Notice on The Ministry of Culture and Various Departments' Opinion on Regulations For Developing Internet Cafes and other Places of Business for the Provision of Internet Access Services] (promulgated by the St. Council, Feb. 17, 2004), <http://w.51sobu.com/policy/39043172004314261080281968453.html> (last visited Feb. 13, 2006) (P.R.C.); See also *Zhonggong zhongyang guowu yuan guan yu jin yi bu jia qiang he gai jin wei cheng nian ren si xiang dao de jian she de ruo gan yi jian* [State Council Opinion on Further Strengthening and Improving the Morality and Ideology of Non-Adults] (promulgated by the St. Council, Feb. 26, 2004), www.ccyl.org.cn/ywdd/files/ywdd20040323.htm (last visited Feb. 13, 2006) (P.R.C.).

92. *Wen hua bu guan yu jia qiang chun jie han jia qi jian hu lian wang shang wang fu wu ying ye chang suo guan li gong zuo de jin ji tong zhi* [Ministry of Culture, Urgent Notice on Tighter Regulation on the Manage-

install software to filter out more than 500,000 banned sites that are considered by the authorities to be offensive or subversive.⁹³

In parallel to this scheme, Internet publishers, Web portals, and Web managers are also required to shoulder monitoring duties under the *Interim Provisions on the Administration of Internet Publication* of 2002.⁹⁴ Under article 5 of the *Provisions*, Internet publishing is defined as “online transmission acts by Internet information service providers of posting on the Internet, or sending to user terminals through the Internet, after selection and editing, works created by themselves or others for browsing, reading, use or downloading by the public.”⁹⁵ Approval must be obtained for Internet publishing activities (article 6), and Internet publishers are required to keep a record of any works that are posted or transmitted and the time of posting or transmission. Copies must be kept for sixty days and be provided to the relevant authorities on request (article 22). Editors are held responsible for the “legality of content,” meaning that all content must be examined and reviewed (article 21). Those working for Internet publishers are required to undergo “training” before assuming their duties (article 21).⁹⁶ Advance filing with the relevant government departments of all content “concerning national security or social stability” is also required (article 16). Punishment for the violation of the *Provisions* ranges from fines and the confiscation of property and income to suspension of licenses and closure.⁹⁷ In March 2005, the authorities announced that all owners of personal Web sites, Webmasters of bulletin boards, and Web logs (blogs) must register with the government by June 2005,⁹⁸

ment of Places of Business for the Provision of Internet Access Services During Spring Festival and Winter Break] (promulgated by the Min. Cult., Jan. 12, 2004, effective Jan. 12, 2004) http://www.ccm.gov.cn/zcfg/last_zcfgo.jsp?id=389 (last visited Feb. 8, 2006) (P.R.C.).

93. Qiang, *supra* note 5, at 71.

94. Interim Internet Publications Provisions, *supra* note 11.

95. *Id.* art. 5.

96. For further discussion of the Provisions, see Mitch Dudek, Beth Bun nell & Steve Guangyu Yu, *Internet Publishing: China Pushes for Increased Supervision and Self-Discipline in the Industry*, CHINA L. & PRAC., Sept. 2002, at 22-25.

97. See Interim Provisions on the Administration of Internet Publication, *supra* note 11.

98. See Xin xi chan ye bu ICP/IP di zhi xin xi bei an guan li xi tong: chang jian wen ti jie da [Ministry of Information Industry ICP/IP Address

R

R

R

with violators risking a heavy fine or closure of their sites. In September 2005, the government imposed further duties on Internet news information services, covering electronic bulletin services, website managers and bloggers under the *Provisions for the Administration of Internet News Information Services*.⁹⁹ Other than forbidding the dissemination of information that falls under one of the ten categories mentioned in Part IIIA of this article, article 19 of the *Provisions* adds that it is against the law to transmit information on any electronic bulletin service that instigates others to hold any assembly, to form any association or to demonstrate in any unlawful manner; or to organize activities carried out in the name of an illegal non-government organization.¹⁰⁰ The Internet news information service provider must immediately delete such content, keep the records and inform the relevant government department.¹⁰¹ If the provider fails to do so, the government will shut down the Web site(s), and the person responsible for the failure may have to pay a fine up to RMB\$30,000 (about US\$3800).¹⁰² These stern rules show that the government is determined to assign greater responsibility to Internet providers and to enlist them in its policing efforts.

The same standard also applies to providers of Internet cultural products, which are defined under article 2 of the *Interim Provisions on the Administration of Internet Culture* to be Internet entities that produce, disseminate, or circulate audio and video products, game products, show plays, works of art, cartoons or other cultural products.¹⁰³ Under article 19 of these *Provisions*, special examiners must be trained to guarantee the lawfulness of Internet cultural products, and article 21 stipulates that records of all such content must be kept for sixty days.

Filing and Registration System: Frequently Asked Questions and Answers] (promulgated by the Min. Info. Indus., Mar., 2004, effective Mar., 2004) <http://www.longmeng.com/icp1.htm> (last visited Feb. 8, 2006) (P.R.C.).

99. Provisions for the Administration of Internet News Information Services, (promulgated by the Min. Info. Indus., Sept. 25, 2005, effective Sept. 25, 2005) art. 2, LAWINFOCHINA (last visited Feb. 7, 2006) (P.R.C.).

100. *Id.* art. 19.

101. *Id.* art. 20.

102. *Id.* art. 27.

103. Interim Provisions on the Administration of Internet Culture, *supra* note 59, art. 2.

Likewise, a similar model has been adopted to govern the publication of audio-visual programs through the Internet. Under article 20 of *the Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network* of 2004,¹⁰⁴ all license-holding institutions must establish their own management and examination systems, including the appointment of a chief editor who is to be responsible for the content of the published audio-video programs. Under article 22 of these *Measures*, the names of the products, outlines of their content, and related information must be kept on record for thirty days, and failure to do so may constitute a crime.

Furthermore, new copyright legislation was enacted in May 2005. Rather than holding the owners or creators of Web sites to be directly responsible for copyright infringement, Internet service providers and Web hosting companies may be held criminally responsible for copyright infringements on the sites that they host. Under article 5 of *the Measures for the Administrative Protection of Internet Copyright*,¹⁰⁵ Internet information service providers must remove the relevant content upon notification by copyright owners of copyright violation, and failure to do so may include administrative penalties. Although this may be reminiscent of the “notice and take down system” that has been adopted in the United States and Europe,¹⁰⁶ criminal liability may also be imposed on IISPs in certain “severe circumstances” that are not defined in the *Measures*.¹⁰⁷

104. *Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or Other Information Network* (promulgated by the St. Admin. Radio, Film & Telev., July 7, 2004, effective Oct. 11, 2004) art. 20, LAWINFOCHINA (last visited Feb. 17, 2006) (P.R.C.).

105. *Measures for the Administrative Protection of Internet Copyright* (promulgated by the St. Bur. Copyright and the Min. Info. Indus., Apr. 30, 2005, effective May 30, 2005) art. 5 LAWINFOCHINA (last visited Feb. 17, 2006) (P.R.C.).

106. See 17 U.S.C. § 512(c)(1)(A)(iii), (c)(1)(C) (1998), Council Directive 2000/31, arts. 12-14, 2000 O.J. (L 178) 1, 12-13 (EC). However, it is important to note that under both the U.S. and the European system, no criminal responsibility is imposed on Internet service providers. 17 U.S.C. § 512(c), Council Directive 2000/31, arts. 12-14, 2000 O.J. (L 178) 1, 12-13 (EC).

107. Under Article 14 of the Measure for the Administrative Protection of Internet Copyright, *supra* note 105, certain government departments may

In sum then, the picture of Internet regulation in China is composed of Internet cafe managers patrolling their own shops and Yahoo! monitoring its own chat rooms and screening the e-mail messages of its users. In addition, all these are overseen by an army of more than 50,000 state cyber-police.¹⁰⁸

IV. PARTNERSHIP BETWEEN GOVERNMENT AND BUSINESS: DANCING WITH WOLVES

The tight grip of the Chinese government means that Internet service and content providers, Internet cafe owners, and Internet users operate in a repressive environment, and it could easily be concluded that conducting Internet-related business in China is not an attractive option. However, many foreign investors have had their eyes on the Chinese Internet market for a long time. The population of netizens in China is the second largest in the world after the United States, and the potential of the Chinese market became even more promising after China signed a bilateral accession protocol with the United States in November 1999.¹⁰⁹ Under this agreement, China will allow 30% foreign ownership of telecommunications firms upon accession to the WTO, 49% after the first year, and 50% after the second year.¹¹⁰ The telecommunications industry also includes the Internet sector, and as China formally became a member of the WTO in 2001, the prospect of attracting foreign Internet investors is favorable.¹¹¹ In 2004, the government gave the green light for foreign investment in

punish IISPs under other severe circumstances, and under article 16 it is clearly stated that the criminal liability of IISPs shall be decided by the court.

108. Howard W. French, *Chinese Censors and Web Users Match Wits*, N.Y. TIMES, Mar. 4, 2005, at A10.

109. See White House Office of Public Liaison, *Summary of U.S.-China Bilateral WTO Agreement*, <http://clinton4.nara.gov/WH/New/WTO-Conf-1999/factsheets/fs-006.html> (signed on Nov. 15, 1999). For a summary of the details, see Press Release, Office of the United States Trade Representative, *USTR on Shanghai Talks on China's Accession to WTO*, (June 14, 2001), <http://www.usconsulate.org.hk/uscn/trade/general/ustr/2001/061401.htm>.

110. See White House Office of Public Liaison, *Briefing on the Clinton Administration Agenda for the World Trade Organization Material, Summary of U.S.-China Bilateral WTO Agreement* (Nov. 17, 1999), available at <http://www.uschina.org/public/991115a.html> (last visited Feb. 17, 2006).

111. See Peter K. Yu, *Barriers to Foreign Investment in the Chinese Internet Industry* (Mar. 2001), GIGALAW, Mar. 2001, <http://www.gigalaw.com/articles/2001-all/yu-2001-03-all.html>.

television program production.¹¹² In 2005, the State Council announced that investment of privately owned capital in the cultural sector is encouraged; this sector includes places of business that provide internet access services, and animated and online games industry.¹¹³ It is explicitly stipulated that privately owned capital cannot be invested in news agencies.¹¹⁴ Content regulation is likely to remain the same, with Internet connections are still being prevented from linking with overseas Web sites or carrying news information from overseas sites.¹¹⁵

Though uncertainty remains, this has not deterred foreign investors. In 2000, AT&T established a joint venture with China Telecom in Shanghai, and in late February 2001 China Netcom was able to raise \$325 million from private investors.¹¹⁶ In 2003, SK Telecom, a South Korean company, signed a deal with state-run China Unicom Ltd. to provide value-added services to wireless phones.¹¹⁷ British Vodafone Group PLC successfully secured a 3.3% stake in China Mobile

112. See *Provisional Measures Governing the Administration of Sino-Foreign Equity and Cooperative Joint Ventures that Produce and Operate Radio and Television Programmes* (promulgated by the St. Admin. of Radio, Film & Telev. and the Ministry of Commerce, Oct. 28, 2004, effective Nov. 28, 2004) (P.R.C.), available at http://www.tdctrade.com/report/reg/reg_050303.htm. For a discussion of these *Provisions*, see Jeanette K. Chan and Marcia Ellis, *Foreign Media, Chinese TV and Market Access: The New Rules from SARFT, CHINA L. & PRAC.*, Dec. 2004, available at <http://www.chinalawandpractice.com>.

113. Entry into the Cultural Sector of Non-Publicly Owned Capital Several Decisions (promulgated by the St. Council, Apr. 13, 2005), CHINALAWANDPRACTICE (P.R.C.). Non-publicly owned capital is understood to include foreign enterprises, according to an explanatory note reported in the state media. See *Several Decisions by the State Council on Non-Publicly Owned Capital's Entry into the Cultural Sector* [Guowu yuan guan yu fei gong you zi ben jin ru wen hua chan ye de ruo gan jue ding], CCTV CHANNEL, Aug. 8, 2005, <http://www.cctv.com/news/china/20050808/102504.shtml>.

114. Entry into the Cultural Sector of Non-Publicly Owned Capital Several Decisions, art. 9, *supra* note 113.

115. C.f. Chin-Chuan Lee, *supra* note 16, at 12-13 (for an analysis of the situation in 2003; at the time that this article was written, the situation remains the same.)

116. Tao & Wang, *supra* note 82.

117. Rebecca Buckman, *China's Mixed Telecom Signals—Market Openings Have Done Little to Boost Foreign Investment*, ASIAN WALL ST. J., Dec. 7, 2004, at A3.

R

R

R

(Hong Kong) Ltd.¹¹⁸ Motorola became China's fourth largest foreign investor with exports exceeding US\$3 billion and Nokia exceeding US\$2 billion.¹¹⁹ In 2004, Russian Telecom formed an agreement with China Telecom to build an inter-city fiber-optic system.¹²⁰ Although foreign investors may view the Chinese authorities as controlling, unpredictable, and arbitrary, the profit potential in the Chinese market is enormous. The Chinese media have described the liaison between China's telecommunications industry and global capital as "dancing with wolves."¹²¹

Each side is well aware that the other is difficult to tame. The Chinese government knows that its electronic panopticon surveillance model that is based on the Benthamite and Foucauldian theories of direct discipline and indirect monitoring may not work, and that the most effective and powerful means of exerting power is through co-optation, a process of bringing in and absorbing outsiders so that they fall in line with the central authority and no longer pose a threat to the organization's stability or existence.¹²² In effect, the authorities must successfully woo foreign investors to join their team, but cooperation can only be based on the common interest of economic benefits. The close alliance between the Chinese authorities and foreign investors is being forged through the construction of an Internet security system and the development of the e-market.

A. Partnership in Building a Cyber-Panopticon

Before China opened its Internet sector to foreign investors and devised its elaborate system of indirect control, the development of Internet technology in China had already been infiltrated by foreign high-tech firms. The sheer size of

118. *Id.*

119. Hanika Damodharan, *Chinese Telecom: Trends in Foreign Investments*, FROST & SULLIVAN MARKET INSIGHT, July 8, 2005, <http://www.frost.com>.

120. Press Release, China Telecom, Fr. People's Post & Telecommunications News, (July 20, 2004), http://new.huaosico.com/news_e/news_e3_115.htm.

121. Yuezhi Zhao & Dan Schiller, *Dances with Wolves? China's Integration into Digital Capitalism*, 3 J. POL'Y, REG. & STRATEGY FOR TELECOMM. INFO. & MEDIA 137, 146 (2001).

122. JOSEPH MAN CHAN & CHIN-CHUAN LEE, MASS MEDIA AND POLITICAL TRANSITION 33 (1991).

the government project is lucrative enough for foreign firms to put aside the Internet vision of democracy and citizen empowerment, and thus the technology that is being used to open up the world is also being used to narrow it.

In addition to network routers and switches, Cisco is known in the West for building corporate firewalls to block viruses and hackers,¹²³ but it is also the builder of the great firewall in China. Working directly under the supervision of State Security, the Public Security Bureau, and the People's Liberation Army, its technology was responsible for a specially designed router device, integrator, and firewall box for the government's telecom monopoly.¹²⁴ The cost of each box is believed to be about US\$20,000, and China Telecom bought many thousands from Cisco.¹²⁵ The project was financed by IBM.¹²⁶ Cisco has also helped the Chinese government to monitor e-mail and other packets of data. In 2004, Cisco secured a contract worth more than US\$100 million with China Telecom to build a new backbone network to link two hundred Chinese cities,¹²⁷ and was also chosen to be the main provider of equipment for ChinaNet, the country's largest public network.¹²⁸

Microsoft proxy servers have been used to block Web pages.¹²⁹ In December 1996, Sun Microsystems obtained a US\$15 million deal to build the Intranet backbone of the Chinese worldwide Web,¹³⁰ and helped the government compile a nationwide database of fingerprints. In January 1997, Bay Networks (now Nortel) won a bid to build a multi-million dollar infrastructure.¹³¹ Websense has contributed to sophisticated Internet monitoring and filtering techniques, and Nortel played a major part in developing a system whereby surveil-

123. See PC World Business – Taking Care of Your Business, <http://www.pcwb.com/showcases/cisco>.

124. See Ethan Gutmann, *Who Lost China's Internet?*, 7 WEEKLY STANDARD, Feb. 25, 2002, at 25.

125. *Id.*

126. See *id.* at 24-25.

127. Tom Zeller, Jr., *Beijing Loves the Web Until the Web Talks Back*, N.Y. TIMES, Dec. 6, 2004, at C15.

128. *Id.*

129. Qiu, *supra* note 30, at 11.

130. *Id.*

131. *Id.*

lance data can be transferred from CCTV cameras along the country's railway network to a centralized point in the Ministry of Public Security.¹³² Nortel has worked with Tsinghua University to develop speech recognition software, and has developed a prototype fiber-optic network with firewalls that enables the government to track the surfing habits of Internet users.¹³³ Nortel also provided software for voice and closed-circuit camera recognition technology to the Public Security Bureau.¹³⁴ iCognito, an Israeli company that invented a program called "artificial content recognition" that can surf ahead of the user and censor information in real time, has targeted China Telecom as a potential customer.¹³⁵

The 2000 Security China Fair was dominated by Cisco, Sun, and Nortel.¹³⁶ In 2003, Nielsen/NetRatings secured the first and only service by the Chinese government to measure the behavior of Internet consumers and will offer services that track Internet audiences and advertising activity in China on a monthly basis.¹³⁷ Nielsen/NetRatings has promised to adhere to all of the regulations and policies of the Chinese government and to ensure the integrity of its Internet measurement information.¹³⁸

In the midst of this growing alliance between the Chinese government and high-tech firms, some have called for "boar-droom consciousness" and "corporate ethics."¹³⁹ The involved companies, however, defend their activities and their roles as being the same as designing guns or building airplanes. They have the technology, and are not concerned with how these

132. The information in this paragraph is taken from David Lee, *Multinationals Making a Mint from China's Great Firewall*, S. CHINA MORNING POST, Oct. 2, 2002, at 16.

133. *Id.*

134. *Id.*

135. Gutmann, *supra* note 124, at 26.

136. Wacker, *supra* note 12, at 69.

137. *Nielsen Receives Government Approval to Conduct Internet Tracking Research in China*, WORLD IT REP., Apr. 9, 2003, at 1.

138. *Id.*

139. These include the International Centre for Human Rights and Democracy, Human Rights Watch, and Professor Ralph Steinhardt at the George Washington University Law School. *See* Lee, *supra* note 132.

R

R

R

products will be used after they are purchased.¹⁴⁰ Companies perceive themselves as mere conduits, empty vessels that do not hold any values. However, when mainland journalist Shi Tao was sentenced to ten years of imprisonment for “divulging state secrets abroad” in April 2005, Yahoo! was condemned as a Chinese “police informant” and collaborator,¹⁴¹ because it had passed detailed information of Shi Tao’s e-mail correspondence to the China’s state security authorities.¹⁴² Yahoo! defended its action by explaining that the company had no alternative but to follow the law in China.¹⁴³ Otherwise, its executives would face serious legal sanctions.¹⁴⁴ Though Yahoo! is different from a high tech company in many ways, that its willingness to cooperate with the authorities led to the conviction of a journalist warrants serious concern from the international community. The claim that a company is an entirely neutral agent that may sacrifice its customers’ privacy and freedom is hardly convincing to many customers. The entire debate on corporate ethics, seeking profits, and appeasing authoritarian government may better be viewed in light of universal human rights standards.

But without going further into this debate on business ethics, it can be asserted that the Internet technology of overseas companies has played a definitive role in shaping China’s Internet development, despite their singular goal of reaping profits.

140. The replies came from Cisco’s systems engineer manager and Nortel’s spokeswoman. *See* Gutmann, *supra* note 126, at 25; Lee, *supra* note 132.

R
R

141. Press Release, Reporters Without Borders, Information Supplied by Yahoo! Helped Journalist Shi Tao Get 10 Years in Prison, Sept. 6, 2005, http://www.rsf.org/print.php3?id_article=14884 (last visited Feb. 17, 2006).

142. Shi Tao worked for the Contemporary Business News (Dangdai Shang Bao). He sent a message to foreign websites concerning an internal government message that warned journalists of the dangers of social destabilization and risks resulting from the return of certain dissidents on the fifteenth anniversary of the Tiananmen Student Movement. For the judgment, see Crim. Div. One, First Trial Case No. 29 (Changsha Interim. People’s Ct. of Hunan Province, Apr. 27, 2005), *available at* http://www.rsf.org/IMG/pdf/Verdict_Shi_Tao.pdf.

143. Michael Logan, Bien Perez & Jamil Anderlini, *Boycott Threat Shames Yahoo – Case of Imprisoned China Journalist Highlights Risks for Net Companies Operating in the Mainland*, S. CHINA MORNING POST, Sept. 13, 2005, at 1.

144. *See id.*

B. *A Business Culture of Self-Censorship*

Although foreign investors are more interested in e-commerce than Internet content, they are likely to try to avoid any unintended violations of Internet regulations in China. Self-censorship was evident during the 2000 Taiwan elections,¹⁴⁵ and Sparkice, a Canadian Internet company, announced that it would feature only state-sanctioned news on its Web site.¹⁴⁶ Yahoo! has been criticized for offering sanitized messages on its Chinese Web site, and it has been reported that keying in the words “Falun Gong” in Yahoo! yields only one result: a condemnation from officials.¹⁴⁷ Thus, it would appear that Internet service and content providers have largely complied with the principle of “no sex, no violence, and no news.”

As of June 2005, mainland users of Microsoft’s MSN blog service were unable to use a list of “forbidden words,” that include “democracy,” “freedom,” “Taiwan independence,” and “demonstration.”¹⁴⁸ Entering these words only prompts an error message. While Human Rights Watch condemned this to be a blatant form of “electronic kowtow,”¹⁴⁹ a reader of a newspaper pointed out the ironic and ridiculous situation that Mao Zedong’s famous essay “On New Democracy” would also be censored in Microsoft MSN.¹⁵⁰ On the business side, Microsoft has managed to be the first big international Internet service provider to win a license for value-added telecom services in China.¹⁵¹

Without prompting, in March 2002, the China Internet Industry initiated the “voluntary” Public Pledge of Self-Discipline for China Internet Industry, article 9 of which states that signatories are required to “monitor the information publi-

145. Xiangmin Xu & Hu Zaichi, *China’s Internet Sector: A Regulatory Overview*, INT’L INTERNET L. REV., Apr. 2000, at 32.

146. Gutmann, *supra* note 126, at 26.

147. See *Stop Your Searching*, ECONOMIST, Sept. 7, 2002.

148. *No to Freedom: Microsoft’s Self-Censorship in China is Self-Defeating*, FIN. TIMES, June 15, 2005, at 18.

149. See Editorial, *The Electronic Kowtow*, ASIAN WALL ST. J., June 15, 2005, at A11. “Kowtow” means “to bow” in Chinese.

150. Arthur Waldron, Letter to the Editor, *Internet Censorship Shows that Business Will Have to Learn to Play by Chinese Rules*, FIN. TIMES, June 17, 2005, at 18.

151. Mure Dickie, *Don’t Mention Democracy, Microsoft Tells Chinese Web Users*, FIN. TIMES, June 11, 2005, at 8.

cized by users on Web sites according to [Chinese] law and remove the harmful information promptly.”¹⁵² In addition, signatories are also required to refrain from “establishing links to Web sites that contain harmful information so as to ensure that the content of the network information is lawful and healthy.”¹⁵³ More than one hundred Internet companies or Internet-related companies voluntarily signed the Public Pledge when it was first launched,¹⁵⁴ including Yahoo!, Sinanet, and Sohu.¹⁵⁵ By July 2002, more than three hundred companies had signed the Pledge,¹⁵⁶ and these businesses will essentially act as “little brothers” in policing Internet messages. The implicit bargain appears to be that, in exchange, their smooth operation in China will be guaranteed.

The fate of those businesses that have not signed is uncertain. The Google and AltaVista sites were temporarily closed by the Chinese government at the end of August 2002, and although the Google site reopened in September 2002, the government never offered an explanation for the closure.¹⁵⁷ From the outset the ban was never announced, and it was not apparent what Google had done to provoke or offend the Chinese government. The general belief was that the government had attempted to maintain a clean Internet environment in the run-up to the 16th Communist Party Congress in November.¹⁵⁸ Google has enjoyed great popularity in China, not only because it allows users to search for pages in simplified Chi-

152. Internet Society of China, Public Pledge on Self-Discipline and Professional Ethics for China Internet Industry, Mar. 28, 2002, *available at* www.isc.org.cn/20020417/ca102762.htm. The Internet Society of China is supported by the Chinese government.

153. *Id.* art. 9, cl. 2.

154. *China's Internet Industry Wants Self-Discipline*, People's Daily, March 26, 2002, *available at* http://english.peopledaily.com.cn/200203/26/print20020326_92885.html (last visited Feb. 17, 2006).

155. *See* Press Release, U.S. State Dep't, Human Rights Abuses Systematic Problem for China (Apr. 14, 2005), <http://usinfo.state.gov/eap/Archive/2005/Apr/15-538552.html> (last visited Mar. 20, 2006).

156. Amnesty International, PEOPLE'S REPUBLIC OF CHINA: STATE CONTROL OF THE INTERNET OF CHINA 12 (2002), *available at* [http://web.amnesty.org/library/pdf/ASA170072002ENGLISH/\\$File/ASA1700702.pdf](http://web.amnesty.org/library/pdf/ASA170072002ENGLISH/$File/ASA1700702.pdf).

157. *See* Benjamin Edelman, *When the Net Goes Dark and Silent*, South China Morning Post, Oct. 2, 2002.

158. *See* Catherine Armitage, *China Censors Bowl Net Users a Googly*, THE AUSTRALIAN, Sept. 5, 2002, at 7.

nese characters,¹⁵⁹ but also because it can link to Web pages that are stored on Google's computers, which means that even if a server is blocked one can still gain access to its content.¹⁶⁰ However, after the Google site was restored the Chinese government installed a new filter system to make it difficult to use Google to search for materials that are deemed offensive.¹⁶¹

Google has learned its lesson well, and as of 2004, has decided to omit sources from its Google News China edition that the authorities may not like.¹⁶² Sites that are censored by Google include The Epoch Times and Dynamic Internet Technology.¹⁶³ While Google did not deny banning certain sensitive sites, it claimed that this policy was to improve the quality and efficiency of its search engine, because to include government banned sites would only damage the user interface experience.¹⁶⁴ The company explained that Google China users would feel frustrated just to see results and links and yet be unable to click through to the actual pages.¹⁶⁵ Regardless of whether one finds Google's explanation convincing, the objective fact is that in the same year, Google successfully formed a

159. Michael Logan & Sidney Luk, *CHINA: Google Homes in on Mainland*, ASIA MEDIA, May 6, 2004, available at <http://www.asiamedia.ucla.edu/article.asp?parentid=10900> (last visited Mar. 23, 2006).

160. See Stephanie Olsen, *Google cache raises copyright concerns*, CNET News, July 9, 2003, http://news.com.com/2100-1038_3-1024234.html.

161. *Google Censors Itself for China*, BBC News, Jan. 25, 2006, available at <http://news.bbc.co.uk/1/hi/technology/4645596.stm> (last visited Mar. 21, 2006).

162. Google adopted this policy in October 2004. See *The Electronic Kowtow*, ASIAN WALL ST. J., June 15, 2005, at A11.

163. See Simon Thomas, *Keep Searching: The Epoch Times Not Welcome on Google*, THE EPOCH TIMES, Sept. 25, 2004, available at <http://www.theepochtimes.com/news/4-9-25/23439.html>. Dynamic Internet Technology is an American company that provides technology for circumventing Internet restrictions in China. Will Knight, *Google Omits Controversial News Stories in China*, NEW SCIENTIST, Sept. 21, 2004, <http://www.newscientist.com/article.ns?id=DN6426>. The Epoch Times is closely related to spiritual group Falun Gong, which is banned in China and condemned as an evil cult by the Chinese government. See Michael Ng, *Falun Gong-linked paper facing closure*, THE STANDARD (Hong Kong), May 12, 2005, available at <http://www.thestandard.com.hk/stdn/std/Metro/GE12Ak01.html>.

164. Simon English, *Google Accused of Aiding Chinese Censors*, DAILY TELEGRAPH (London), Sept. 27, 2004, at 27.

165. *Id.*

partnership with Baidu, one of the most popular search engines in China.¹⁶⁶

Others who have dared to test the boundaries have had to pay a price. It is believed that the *New York Times* Web site was banned until it published a lengthy interview with the then President Jiang Zemin,¹⁶⁷ and the China Finance Information Network was suspended for fifteen days and fined RMB\$15,000 (about US\$1900) for republishing a Hong Kong newspaper article about corruption by a provincial official.¹⁶⁸

However, to be truly competitive in the Chinese e-market, it may not be enough to be duly compliant: that extra step of voluntary self-censorship must be taken before the intervention of formal censorship.

C. *Exception to the Rule*

If self-censorship is necessary for survival, then it can only go so far to serve the interests of investors. Few if any of the foreign capitalists have protested against the Chinese government's attempt to control and regulate the Internet, nor do they oppose the stringent controls on monitoring and reporting. A raw nerve was, however, immediately touched in 1999 by the *Encryption Regulations*. The Chinese government considers encryption technology to fall within the definition of state secret,¹⁶⁹ but such technology is essential to the running of e-commerce and is embedded in the design of many software programs.¹⁷⁰ Encryption technology is also indispensable for multinational corporations to be able to communicate information securely across distributed networks. However, advanced encryption products are difficult or impossible to crack, which thus undermines the ability of the state to monitor communications.¹⁷¹ The *Encryption Regulations*, by demanding that all Western firms that are based in China use Chinese technology, gives the Chinese government access to

166. Zeller, *supra* note 127.

167. See Wacker, *supra* note 12, at 66.

168. *China Shuts Down Financial Web Site*, Digital Freedom Network (May 15, 2000), available at dfn.org/focus/china/cfinet.htm.

169. Encryption Regulations, *supra* note 63, art. 3 ("Commercial encryption technology is a State secret.").

170. Deibert, *supra* note 36, at 151.

171. *Id.*

R

R

R

R

industrial secrets. Microsoft vehemently opposed the *Encryption Regulations*, and many multinational companies that produce, sell, or use encryption products, together with the chambers of commerce of various countries,¹⁷² staged a campaign against the *Regulations*. Eventually, the government clarified in March 2000 that the *Encryption Regulations* only covered those types of specialist hardware and software in which encryption and decoding operations are core functions, but not other products that contain encryption codes, such as mobile telephones, Windows software, and browser software.¹⁷³ Nevertheless, Microsoft was forced to delay the launch of its Windows 2000 operating system in China as a result of this situation.¹⁷⁴

V. CONCLUSION

At the dawn of the Internet age, many had utopian hopes that it would trigger a new wave of worldwide democracy.¹⁷⁵ In this age of digitalization, many still adhere to the belief and cherish the dream that the Internet will eventually bring forth borderless, open government. Although the power and the potential of the Internet are beyond dispute, we must be cautious not to over-romanticize this “new wild west,” and scholars warn us that “new technology alone is not enough to guarantee an improving public sphere.”¹⁷⁶

172. These included the American Chamber of Commerce, the China Japanese Chamber of Commerce and Industry, German Chamber of Commerce in China, the French Chamber of Commerce, and the e-Commerce China Forum. See Tibor Baranski & Taili Wang, *The Chinese-Chinese-Foreign Incident of China Unicom*, CHINA L. & PRAC., Dec. 2000, available at 2000 WLNR 261668 (Westlaw).

173. The clarification was issued by the State Encryption Management Commission General Office in March 2000. For the English version, see Unofficial Translation by the US-China Business Council of the Document issued March 2000 by the SEMC, available at www.uschina.org/press/000314.html. For a further discussion of this issue, see also Hu Zaichi, *supra* note 67, at 33.

174. See Adam Creed, *Microsoft Launches Windows 2000 in China*, NEWSBYTES, Mar. 20, 2000; Deibert, *supra* note 36, at 151.

175. See, e.g. HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993); CYBERDEMOCRACY: TECHNOLOGY, CITIES AND CIVIC NETWORKS (Roza Tsagarousianou, Damian Tambini & Cathy Bryan eds., 1998).

176. Barrett L. McCormick & Qing Liu, *Globalization and the Chinese Media: Technologies, Content, Commerce and the Prospects for the Public Sphere*, in CHINESE MEDIA, GLOBAL CONTEXTS 139, 154 (Chin-Chuan Lee ed., Routledge 2003).

R

R

As can be seen from the Chinese story, Internet content control has been built on a mixture of legal regulations, technology, and commercialization. The waves of legislation that have been passed in China to monitor the Internet have caused a ripple effect in legal, Internet, and business culture, and concrete legal regulations on the suppression of speech are going hand in hand with an emerging set of social business norms.

Although the free flow of information is essential to business operations, the goal of increasing profits almost always overrides the virtues of civil liberties in China. Foreign capitalists have provided technology to limit access to information and to facilitate the government surveillance of Internet users, and in doing so have voluntarily transformed themselves from information gateways to information gatekeepers.¹⁷⁷ Only when self-interest is directly at stake do they speak up. Saskia Sassen, writing in the context of globalization in the late 1990s, already pointed out that the commercialization of the Internet may in fact dampen its democratic impact.¹⁷⁸ Corporate forces have immense power to shape the digital network, but whether they enable us to build a utopian broad-based civil society is another matter.

This paper does not intend to sound the death knell for the liberating potential of the Internet. With the increasing commercialization of the Chinese market, the importation of business culture will eventually promote individualism and enterprise autonomy, and will ultimately challenge the official ideology. It is true that it is better to have a Big Brother and Little Brother Internet than no Internet at all, but nevertheless the cyber path to freedom is a long and winding one.

177. See the comments of Kenneth Roth in Press Release, HUM. RTS. WATCH, YAHOO! RISKS ABUSING RIGHTS IN CHINA (2002), <http://hrw.org/press/2002/08/yahoo080902.htm>.

178. Saskia Sassen, *The Impact of the Internet on Sovereignty: Unfounded and Real Worries* (German American Academic Council's Project "Global Networks and Local Values," 1999), available at <http://www.mpp-rdg.mpg.de/dresden1.html>.

